CLAIM AMENDMENTS

1. (Currently Amended) A method for facilitating Internet security protocol (IPsec) based communications through a device that employs address translation in a telecommunications network, the method comprising the steps of:

receiving a first electronic message from a first node, wherein:

the first node is associated with a first network address;

the first electronic message is based on IPsec;

the first electronic message is associated with a first identifier;

the first identifier is a first IPsec Security Parameter Index (SPI);

the first identifier is generated by the first node; and

the first electronic message is addressed to a second network address;

the device generating a value based on the first identifier and a specified scheme, wherein the specified scheme is a computer-implemented operation that is known to both the device that employs address translation and a second node;

sending the first electronic message to [[a]] the second node based on the second network address, wherein the first electronic message includes a particular network address that is associated with the device instead of the first network address;

receiving a second electronic message from the second node, wherein:

the second electronic message is based on IPsec;

the second electronic message is addressed to the particular network address;

the second electronic message is associated with a second identifier that is different than the first identifier; ~~and~~

the second identifier is a second IPsec SPI; and

the second identifier is generated, based on the first identifier and the specified scheme, by the second node;

the device determining whether the second electronic message is directed to the first node based on the value and the second identifier; and

sending the second electronic message to the first node at the first network address when the second electronic message is determined to be directed to the first node.

2. (Currently Amended) A method as recited in claim 1, further comprising the steps of:

receiving a third electronic message from a third node, wherein:

the third node is associated with a third network address;

the third electronic message is based on IPsec;

the third electronic message is associated with a third identifier;

the third identifier is a third IPsec SPI; and

the third identifier is generated by the third node; and

the third electronic message is addressed to the second network address;

the device generating an additional value based on the third identifier and the specified scheme;

sending the third electronic message to the second node based on the second network address, wherein the first electronic message includes the particular network address that is associated with the device instead of the third network address;

receiving, after sending the first electronic message and the third electronic message to the second node, the second electronic message from the second node;

wherein:

the second electronic message is based on IPsec;

the second electronic message is addressed to the third network address;

the second electronic message is associated with the second identifier that is different than the first identifier and the third identifier; and

the second identifier is generated, based on the third identifier and the specified scheme, by the second node;

the device determining whether the second electronic message is directed to the third node based on the additional value and the second identifier; and

when the second electronic message is determined to be directed to the third node, sending the second electronic message to the third node at the third network address.

3. (Cancelled)

4. (Previously Presented) A method as recited in claim 1, wherein the specified scheme is selected from the group consisting of a first scheme that produces a fixed length output, a second scheme that includes a hash algorithm, and a third scheme that includes a Message Digest 5 one-way hash function.

5. (Cancelled)

6. (Cancelled)

7. (Cancelled)

8. (Cancelled)

9. (Previously Presented) A method as recited in claim 1, wherein:
the value is a hash value;
the second identifier is based at least in part on the hash value;
the hash value is comprised of a first plurality of bytes;
the second identifier is comprised of a second plurality of bytes;
a last pair of bytes of the second plurality of bytes is a first pair of bytes of the first plurality of bytes; and
the step of determining whether the second electronic message is directed to the first node further comprises the steps of:
comparing the last pair of bytes of the second identifier to the first pair of bytes of the hash value; and
when the last pair of bytes of the second identifier match the firs pair of bytes of the hash value, determining that the second electronic message is directed to the first node.

10. (Currently Amended) A method as recited in claim 1, wherein:
the first node is an IPsec originator node;
the second node is an IPsec responder node;

~~the first identifier is a first IPsec security parameter index;~~

~~the second identifier is a second IPsec security parameter index;~~

the device employs a feature selected from the group consisting of network address translation (NAT), dynamic address NAT, and network address port translation (NAPT);

and the method further comprises the steps of:

creating and storing a mapping between the value and the first IPsec SPI; ~~security parameter index;~~

creating an association between the value and the first IPsec SPI; ~~identifier;~~ and

storing the association in a translation table.

11. (Previously Presented) A method as recited in claim 1, wherein the first electronic message and the second electronic message are both based on an IPsec feature selected from the group consisting of IPsec tunnel mode and IPsec Encapsulation Security Payload.

12. (Cancelled)

13. (Cancelled)

14. (Cancelled)

15. (Cancelled)

16. (Previously Presented) A method as recited in claim 1, further comprising the steps of:

when the second electronic message is determined to be directed to the first node, creating an association between the first network address and the second identifier;

storing the association in a table;

receiving a third electronic message from the second node, wherein the third electronic message is based on IPsec and is associated with the second identifier; and

determining that the third electronic message is directed to the first node based on the association.

17. (Cancelled)

18. (Currently Amended) A method as recited in claim 1, further comprising the steps of:

receiving a third electronic from the second node, wherein:

the third electronic message is based on IPsec;

the third electronic message is addressed to the specified network address;

the third electronic message is associated with a third identifier that is different than both the first identifier and the second identifier;

the third identifier is a third IPsec SPI; and

the third identifier is generated, based on the first identifier and the specified scheme, by the second node;

the device determining whether the third electronic message is directed to the first node based on the value and the third identifier; and

when the third electronic message is determined to be directed to the first node, sending the third electronic message to the first node at the first network address.

19. (Previously Presented) A method as recited in claim 1, wherein the step of the device generating the value is performed before the step of receiving the second electronic message.

20. (Previously Presented) A method as recited in claim 1, wherein the step of the device generating the value is performed after the step of receiving the second electronic message.

21. (Cancelled)

22. (Cancelled)

23. (Cancelled)

24. (Currently Amended) A method for facilitating Internet security protocol (IPsec) based communications through a device that employs address translation in a telecommunications network, the method comprising the steps of:

receiving a first electronic message from a first node, wherein:

the first node is associated with a first network address;

the first electronic message is based on IPsec;

the first electronic message is associated with a first identifier;

the first identifier is a first IPsec Security Parameter Index (SPI);

the first identifier is generated by the first node based on a second identifier and a specified scheme;

the specified scheme is a computer-implemented operation that is known to both the device that employs address translation and the first node;

the second identifier is a second IPsec SPI;

the first identifier is different than the second identifier; and

the first electronic message is addressed to a second network address;

sending the first electronic message to a second node based on the second network address, wherein the first electronic message includes a particular network address that is associated with the device instead of the first network address;

receiving a second electronic message from the second node, wherein:

the second electronic message is based on IPsec;

the second electronic message is address to the particular network address;

the second electronic message is associated with the second identifier; and

the second identifier is generated by the second node;

the device generating a value based on the second identifier and the specified scheme;

the device determining whether the second electronic message is directed to the first node based on the value and the first identifier; and

sending the second electronic message to the first node at the first network address when the second electronic message is determined to be directed to the first node.

25. (Currently Amended) An apparatus for facilitating Internet security protocol (IPsec) based communications with a device that employs address translation in a telecommunications network, the apparatus comprising:

a processor; and

one or more stored sequences of instructions which, when executed by the processor, cause the processor to carry out the steps of:

generating a value based on both a first identifier that is associated with a first node and a specified scheme, wherein:

the first identifier is generated by the first node[[,]];

the first identifier is a first IPsec Security Parameter Index (SPI); and

the specified scheme is a computer-implemented operation that is known to both the device that employs address translation and the first node;

the apparatus generating a second identifier based on the value, wherein the second identifier is a second IPsec SPI; ~~and the specified scheme;~~

receiving, from the device that employs address translation, a first electronic message that originates from the first node, wherein:

the first electronic message is based on IPsec;

the first electronic message is associated with the first identifier;

the first electronic message includes a particular network address that is associated with the apparatus instead of a first network address that is associated with the first node; and

the first electronic message is addressed to a second network address that is associated with the second node;

in response to receiving the first electronic message, generating a second electronic message to the first node, wherein:

the second electronic message is based on IPsec;

the second electronic message is associated with the second identifier; and

the second electronic message is addressed to the particular network address;

sending the second electronic message to the device that employs address translation at the particular network address;

wherein the device determines whether the second electronic message is directed to the first node based on the second identifier and the value that is generated by the device based on the first identifier and the specified scheme; and

wherein the device sends the second electronic message to the first node at the first network address when the device determines that the second electronic message is directed to the first node.

26. (Cancelled)

27. (Cancelled)

28. (Currently Amended) An apparatus as recited in claim 25, wherein the value is a hash value, ~~the first identifier is a first IPsec Security Parameter Index (SPI), the second identifier is a second IPsec SPI,~~ and the instructions for generating the second IPsec SPI further comprises one or more stored sequences of instructions which, when executed by the processor, cause the process to carry out the step of generating, prior to receiving the first electronic message, the second IPsec SPI based on the hash value.

29. (Currently Amended) An apparatus as recited in claim 25, wherein the value is a hash value, ~~the first identifier is a first IPsec Security Parameter Index (SPI), the second identifier is a second IPsec SPI,~~ the first IPsec SPI is a first randomly generated fixed length value and the instructions for generating the second IPsec SPI further comprises one or more stored sequences of instructions which, when executed by the processor, cause the process to carry out the step of generating the second IPsec SPI based on at least a first portion of the hash value and a second portion of a second randomly generated fixed length value.

30. (Previously Presented) An apparatus for facilitating Internet security protocol (IPsec) based communications through a router that employs network address translation in a telecommunications network, the apparatus comprising:

a processor; and

one or more stored sequences of instructions which, when executed by the processor, cause the processor to carry out the steps of:

receiving a first electronic message from a first IPsec originator node, wherein:

the first IPsec originator node is associated with a first network address;

the first electronic message is secured using IPsec:

the first electronic message is associated with a first security parameter index (SPI);

the first SPI is generated by the first IPsec originator node; and

the first electronic message is addressed to a third network address;

the router generating a first hash value based on the first SPI and a hash algorithm;

sending the first electronic message to an IPsec responder node based on the third network address, wherein the first electronic message includes a particular network address that is associated with the router instead of the first network address;

receiving a second electronic message from a second IPsec originator node, wherein:

the second IPsec originator node is associated with a second network address;

the second electronic message is secured using IPsec;

the second electronic message is associated with a second SPI;

the second SPI is generated by the second IPsec originator node; and

the second electronic message is address to the third network address;

the router generating a second hash value based on the second SPI and the hash algorithm;

sending the second electronic message to the IPsec responder node based on the third network address, wherein the second electronic message includes the particular network address that is associated with the router instead of the second network address;

after sending the first electronic message and the second electronic message to the IPsec responder node, receiving a third electronic message from the IPsec responder node, wherein:

the third electronic message is secured using IPsec;

the third electronic message is associated with a third SPI that is different than the first SPI and the second SPI;

the third electronic message is addressed to the particular network address;

the third SPI is generated by the IPsec responder node based at least in part on the hash algorithm;

the router determining whether the third electronic message is directed to the first IPsec originator node based on the first hash value and the third SPI;

when the third electronic message is determined to be directed to the first IPsec originator node, sending the third electronic message to the first IPsec originator node at the first network address;

determining whether the third electronic message is directed to the second IPsec originator node based on the second hash value and the third SPI; and

when the third electronic message is determined to be directed to the second IPsec originator node, sending the third electronic message to the second IPsec originator node at the second network address.

31. (Previously Presented) An apparatus as recited in claim 30, wherein the first electronic message is based on IPsec tunnel mode and IPsec Encapsulating Security Payload (ESP), the second electronic message is based on IPsec tunnel mode and IPsec ESP, and the hash algorithm is a Message Digest 5 one-way hash function.

32. (Currently Amended) A computer-readable medium carrying one or more sequences of instructions for facilitating Internet security protocol (IPsec) based communications through a device that employs address translation in a telecommunications network, which instructions, when executed by one or more processors, cause the one or more processors to carry out the steps of:

receiving a first electronic message from a first node, wherein:

the first node is associated with a first address;
the first electronic message is based on IPsec;
the first electronic message is associated with a first identifier;
the first identifier is a first IPsec Security Parameter Index (SPI);
the first identifier is generated by the first node; and
the first electronic message is addressed to a second network address;
the device generating a value based on the first identifier and a specified scheme, wherein the specified scheme is a computer-implemented operation that is known to both the device that employs address translation and a second node;
sending the first electronic message to [[a]] the second node based on the second network address, wherein the first electronic message includes a particular network address that is associated with the device instead of the first network address;
receiving a second electronic message from the second node, wherein:
the second electronic message is based on IPsec[[:]];
the second electronic message is addressed to the particular network address;
the second electronic message is associated with a second identifier that is different than the first identifier;
the second identifier is a second IPsec SPI; and
the second identifier is generated, based on the first identifier and the specified scheme, by the second node;
the device determining whether the second electronic message is directed to the first node based on the value and the second identifier; and
sending the second electronic message to the first node at the first network address when the second electronic message is determined to be directed to the first node.

33. (Currently Amended) An apparatus for ~~for~~ facilitating Internet security protocol (IPsec) based communications while employing address translation in a telecommunications network, comprising:
a processor; and

one or more stored sequences of instructions which, when executed by the processor, cause the processor to carry out the steps of:

receiving a first electronic message from a first node, wherein:

the first node is associated with a first network address;

the first electronic message is based on IPsec;

the first electronic message is associated with a first identifier

the first identifier is a first IPsec Security Parameter Index (SPI);

the first identifier is generated by the first node based on a second identifier and a specified scheme;

the specified scheme is a computer-implemented operation that is known to both the device that employs address translation and the first node;

the second identifier is a second IPsec SPI;

the first identifier is different than the second identifier; and

the first electronic message is addressed to a second network address;

sending the first electronic message to a second node based on the second network address, wherein the first electronic message includes a particular network address that is associated with the apparatus instead of the first network address;

receiving a second electronic message from the second node, wherein:

the second electronic message is based on IPsec;

the second electronic message is address to the particular network address;

the second electronic message is associated with the second identifier; and

the second identifier is generated by the second node;

generating a value based on the second identifier and the specified scheme;

determining whether the second electronic message is directed to the first node based on the value and the first identifier; and

sending the second electronic message to the first node at the first network address when the second electronic message is determined to be directed to the first node.

34. (Cancelled)

35. (Currently Amended) An apparatus for facilitating Internet security protocol (IPsec) based communications while employing address translation in a telecommunications network, the apparatus comprising:

means for receiving a first electronic message from a first node, wherein:

the first node is associated with a first network address;

the first electronic message is based on IPsec;

the first electronic message is associated with a first identifier;

the first identifier is a first IPsec Security Parameter Index (SPI);

the first identifier is generated by the first node; and

the first electronic message is addressed to a second network address;

means for generating a value based on the first identifier and a specified scheme, wherein the specified scheme is a computer-implemented operation that is known to both the device that employs address translation and a second node;

means for sending the first electronic message to [[a]] the second node based on the second network address, wherein the first electronic message includes a particular network address that is associated with the apparatus instead of the first network address;

means for receiving a second electronic message from the second node, wherein:

the second electronic message is based on IPsec;

the second electronic message is addressed to the particular network address;

the second electronic message is associated with a second identifier that is different than the first identifier; ~~and~~

the second identifier is a second IPsec SPI; and

the second identifier is generated, based on the first identifier and the specified scheme, by the second node;

means for determining whether the second electronic message is directed to the first node based on the value and the second identifier; and

means for sending the second electronic message to the first node at the first network address when the second electronic message is determined to be directed to the first node.

36. (Currently Amended) An apparatus as recited in claim 35, further comprising:

means for receiving a third electronic message from a third node, wherein:

the third node is associated with a third network address;

the third electronic message is based on IPsec;

the third electronic message is associated with a third identifier;

the third identifier is a third IPsec SPI; and

the third identifier is generated by the third node; and

the third electronic message is addressed to the second network address;

means for generating an additional value based on the third identifier and the specified scheme;

means for sending the third electronic message to the second node based on the second network address, wherein the first electronic message includes the particular network address that is associated with the apparatus instead of the third network address;

means for receiving, after sending the first electronic message and the third electronic message to the second node, the second electronic message from the second node;

wherein:

the second electronic message is based on IPsec;

the second electronic message is addressed to the third network address;

the second electronic message is associated with the second identifier that is different than the first identifier and the third identifier; and

the second identifier is generated, based on the third identifier and the specified scheme, by the second node;

means for determining whether the second electronic message is directed to the third node based on the additional value and the second identifier; and

means for sending the second electronic message to the third node at the third network address, when the second electronic message is determined to be directed to the third node.

37. (Currently Amended) An apparatus as recited in claim 35, wherein the specified scheme is selected from the group consisting of a first scheme that produces a fixed length output, a second scheme that includes a hash algorithm, and a third scheme that includes a Message Digest ~~39~~ 5 one-way hash function.

38. (Previously Presented) An apparatus as recited in claim 35, wherein:
the value is a hash value;
the second identifier is based at least in part on the hash value;
the hash value is comprised of a first plurality of bytes;
the second identifier is comprised of a second plurality of bytes;
a last pair of bytes of the second plurality of bytes is a first pair of bytes of the first plurality of bytes; and
the means for determining whether the second electronic message is directed to the first node further comprises:
means for comparing the last pair of bytes of the second identifier to the first pair of bytes of the hash value; and
means for determining that the second electronic message is directed to the first node, when the last pair of bytes of the second identifier match the firs pair of bytes of the hash value.

39. (Currently Amended) An apparatus as recited in claim 35, wherein:
the first node is an IPsec originator node;
the second node is an IPsec responder node;
~~the first identifier is a first IPsec security parameter index;~~
~~the second identifier is a second IPsec security parameter index;~~
the apparatus employs a feature selected from the group consisting of network address translation (NAT), dynamic address NAT, and network address port translation (NAPT);
and the apparatus further comprises:
means for creating and storing a mapping between the value and the first IPsec SPI; ~~security parameter index;~~

means for creating an association between the value and the first IPsec SPI; ~~identifier;~~ and

means for storing the association in a translation table.

40. (Previously Presented) An apparatus as recited in claim 35, wherein the first electronic message and the second electronic message are both based on an IPsec feature selected from the group consisting of IPsec tunnel mode and IPsec Encapsulation Security Payload.

41. (Previously Presented) An apparatus as recited in claim 35, further comprising:

means for creating an association between the first network address and the second identifier, when the second electronic message is determined to be directed to the first node;

means for storing the association in a table;

means for receiving a third electronic message from the second node, wherein the third electronic message is based on IPsec and is associated with the second identifier; and

means for determining that the third electronic message is directed to the first node based on the association.

42. (Currently Amended) An apparatus as recited in claim 35, further comprising:

means for receiving a third electronic from the second node, wherein:

the third electronic message is based on IPsec;

the third electronic message is addressed to the specified network address;

the third electronic message is associated with a third identifier that is different than both the first identifier and the second identifier;

the third identifier is a third IPsec SPI; and

the third identifier is generated, based on the first identifier and the specified scheme, by the second node;

means for determining whether the third electronic message is directed to the first node based on the value and the third identifier; and

means for sending the third electronic message to the first node at the first network address, when the third electronic message is determined to be directed to the first node.

43. (Previously Presented) An apparatus as recited in claim 35, wherein the value is generated before the second electronic message is received.

44. (Previously Presented) An apparatus as recited in claim 35, wherein the value is generated after the second electronic message is received.

45. (Currently Amended) An apparatus for facilitating Internet security protocol (IPsec) based communications while employing address translation in a telecommunications network, comprising:

a processor; and

one or more stored sequences of instructions which, when executed by the processor, cause the processor to carry out the steps of:

receiving a first electronic message from a first node, wherein:

the first node is associated with a first network address;

the first electronic message is based on IPsec;

the first electronic message is associated with a first identifier;

the first identifier is generated by the first node; and

the first electronic message is addressed to a second network address;

generating a value based on the first identifier and a specified scheme, wherein the specified scheme is a computer-implemented operation that is known to both the device that employs address translation and a second node;

sending the first electronic message to [[a]] the second node based on the second network address, wherein the first electronic message includes a particular network address that is associated with the apparatus instead of the first network address;

receiving a second electronic message from the second node, wherein:

the second electronic message is based on IPsec;

the second electronic message is addressed to the particular network address;

the second electronic message is associated with a second identifier that is different than the first identifier; ~~and~~

the second identifier is a second IPsec SPI; and

the second identifier is generated, based on the first identifier and the specified scheme, by the second node;

determining whether the second electronic message is directed to the first node based on the value and the second identifier; and

sending the second electronic message to the first node at the first network address when the second electronic message is determined to be directed to the first node.

46. (Currently Amended) An apparatus as recited in claim 45, further comprising one or more stored instructions which, when executed by the processor, cause the processor to carry out the steps of:

receiving a third electronic message from a third node, wherein:

the third node is associated with a third network address;

the third electronic message is based on IPsec;

the third electronic message is associated with a third identifier;

the third identifier is a third IPsec SPI; and

the third identifier is generated by the third node; and

the third electronic message is addressed to the second network address;

generating an additional value based on the third identifier and the specified scheme;

sending the third electronic message to the second node based on the second network address, wherein the first electronic message includes the particular network address that is associated with the apparatus instead of the third network address;

receiving, after sending the first electronic message and the third electronic message to the second node, the second electronic message from the second node;

wherein:

the second electronic message is based on IPsec;

the second electronic message is addressed to the third network address;

the second electronic message is associated with the second identifier that is different than the first identifier and the third identifier; and

the second identifier is generated, based on the third identifier and the specified scheme, by the second node;

determining whether the second electronic message is directed to the third node based on the additional value and the second identifier; and

when the second electronic message is determined to be directed to the third node, sending the second electronic message to the third node at the third network address.

47. (Currently Amended) An apparatus as recited in claim 45, wherein the specified scheme is selected from the group consisting of a first scheme that produces a fixed length output, a second scheme that includes a hash algorithm, and a third scheme that includes a Message Digest ~~49~~ 5 one-way hash function.

48. (Previously Presented) An apparatus as recited in claim 45, wherein:

the value is a hash value;

the second identifier is based at least in part on the hash value;

the hash value is comprised of a first plurality of bytes;

the second identifier is comprised of a second plurality of bytes;

a last pair of bytes of the second plurality of bytes is a first pair of bytes of the first plurality of bytes; and

the instructions for determining whether the second electronic message is directed to the first node further comprises one or more stored instructions which, when executed by the processor, cause the processor to carry out the steps of:

comparing the last pair of bytes of the second identifier to the first pair of bytes of the hash value; and

when the last pair of bytes of the second identifier match the firs pair of bytes of the hash value, determining that the second electronic message is directed to the first node.

49. (Currently Amended) An apparatus as recited in claim 45, wherein:
the first node is an IPsec originator node;
the second node is an IPsec responder node;
~~the first identifier is a first IPsec security parameter index;~~
~~the second identifier is a second IPsec security parameter index;~~
the apparatus employs a feature selected from the group consisting of network address translation (NAT), dynamic address NAT, and network address port translation (NAPT);
and the apparatus further comprises one or more stored instructions which, when executed by the processor, cause the processor to carry out the steps of:
creating and storing a mapping between the value and the first IPsec SPI; ~~security parameter index;~~
creating an association between the value and the first IPsec SPI; ~~identifier;~~ and
storing the association in a translation table.

50. (Previously Presented) An apparatus as recited in claim 45, wherein the first electronic message and the second electronic message are both based on an IPsec feature selected from the group consisting of IPsec tunnel mode and IPsec Encapsulation Security Payload.

51. (Previously Presented) An apparatus as recited in claim 45, further comprising one or more stored instructions which, when executed by the processor, cause the processor to carry out the steps of:
when the second electronic message is determined to be directed to the first node, creating an association between the first network address and the second identifier;
storing the association in a table;
receiving a third electronic message from the second node, wherein the third electronic message is based on IPsec and is associated with the second identifier; and

determining that the third electronic message is directed to the first node based on the association.

52. (Currently Amended) An apparatus as recited in claim 45, further comprising one or more stored instructions which, when executed by the processor, cause the processor to carry out the steps of:
receiving a third electronic from the second node, wherein:
the third electronic message is based on IPsec;
the third electronic message is addressed to the specified network address;
the third electronic message is associated with a third identifier that is different than both the first identifier and the second identifier;
the third identifier is a third IPsec SPI; and
the third identifier is generated, based on the first identifier and the specified scheme, by the second node;
determining whether the third electronic message is directed to the first node based on the value and the third identifier; and
when the third electronic message is determined to be directed to the first node, sending the third electronic message to the first node at the first network address.

53. (Previously Presented) An apparatus as recited in claim 45, wherein the value is generated before the second electronic message is received.

54. (Previously Presented) An apparatus as recited in claim 45, wherein the value is generated after the second electronic message is received.